



Principios Generales de la Política corporativa de privacidad y protección de datos

[Marzo 2022]

Control de versiones

Versión	Fecha	Control
1	[28/03/2022]	Revisión y actualización bienal de la Política Adaptación al modelo de Política Corporativa.

Contenido

1. Introducción	4
1.1 <i>Antecedentes</i>	4
1.2 <i>Objetivo</i>	5
2. Ámbito de aplicación	7
3. Marco normativo. Normativa y estándares de aplicación	8
4. Principios generales de la gestión de la privacidad	9
5. Marco de gobierno	10
6. Marco de gestión para la privacidad y la protección de datos	10
6.1 Delegado de Protección de Datos (DPO)	10
6.1.1 Nombramiento	10
6.1.2 Encaje organizativo y funciones	10
6.1.3 Facultades	11
6.1.4 Independencia	12
6.1.5 Disponibilidad y participación efectiva	12
6.1.6 Dotación de medios	12
6.1.7 Comunicación interna y externa en materia de privacidad	12
6.1.8 Relaciones con las funciones de control	13
6.1.9 El Delegado de Protección de Datos Corporativo	13
6.1.10 Modelo de Gobierno de la función de DPO en la presencia internacional	14
6.2 <i>Otras figuras responsables</i>	14
6.2.1 Responsable de Privacidad	14
6.2.2 Coordinador de Privacidad de las Áreas o Direcciones Territoriales	15
6.3 <i>Tratamientos y Legitimación</i>	15
6.4 <i>Derechos de los interesados</i>	15
6.5 <i>Evaluaciones de impacto</i>	15
6.6 <i>Medidas técnicas</i>	16
6.7 <i>Proveedores</i>	16
6.8 <i>Comunicación y formación</i>	16

1. Introducción

1.1 Antecedentes

Caixabank, S.A. es una entidad de crédito, cabecera de un grupo que presta servicios financieros y de inversión (en adelante, “**CaixaBank**” o la “**Entidad**”). Como tal, se ha venido rigiendo por los más altos estándares de respeto al derecho fundamental de protección de datos de carácter personal, así como a la preservación de la confidencialidad de la información que trata. Estos constituyen pilares fundamentales sobre los que se asienta la confianza, valor esencial de su actividad.

En este contexto, el Consejo de Administración de CaixaBank, coincidiendo con el inicio de la aplicación el 25 de mayo de 2018 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante, el “**Reglamento General de Protección de Datos**” o el “**RGPD**”), dio un paso más en su compromiso con la confidencialidad y con la protección de los datos personales estableciendo mediante la política a la que se refieren estos principios (en adelante, la “**Política**”) un marco general de gestión de la privacidad y la protección de datos en la Entidad, adaptada a las nuevas disposiciones normativas y que formalizó la adopción y seguimiento de los principios que la mencionada norma incorpora como son, la privacidad por defecto y por diseño, el enfoque de riesgos y la responsabilidad pro activa.

Asimismo, en abril de 2019 la Comisión Europea publicó las Directrices Éticas para una Inteligencia Artificial fiable, que constituye el primer marco europeo para lograr el uso en la Unión de una inteligencia artificial lícita, ética y robusta. A estas directrices las siguió la publicación en febrero de 2020 del Libro Blanco sobre Inteligencia Artificial: “Un enfoque europeo orientado a la excelencia y la confianza” que plantea la necesidad de establecer un marco regulador europeo de la Ética en el uso de los datos y los sistemas de inteligencia artificial.

Fruto de todo ello, la Comisión Europea, en abril de 2021, publicó su primera propuesta de texto para lo que será el futuro Reglamento Europeo mediante el que se pretenden establecer normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial).

Asimismo, mediante la presente Política, el Consejo de Administración desea establecer los principios que la Entidad y su Grupo aplican en el tratamiento de la información personal, los derechos que reconoce a los Interesados y el marco de gobierno interno del que, en materia de privacidad, quieren dotarse. En la Política a la que se refieren estos principios se regula también la figura del Delegado de Protección de Datos.

Finalmente, el Consejo de Administración con la Política a la que se refieren estos principios pretende garantizar el establecimiento de los procedimientos y medidas necesarias para asegurar una gestión del riesgo de la privacidad acorde con el apetito al riesgo de la Entidad y el Grupo.

El Consejo de Administración tiene la facultad indelegable para la determinación de las políticas y estrategias de la Entidad de acuerdo con el artículo 249 bis del Texto Refundido de la Ley de Sociedades de Capital.

1.2 Objetivo

La Política a la que se refieren estos principios tiene como objetivos:

- Transmitir a todos los/las empleados, directivos y miembros del órgano de administración de la Entidad y del Grupo CaixaBank, el mensaje de que el Grupo vela porque su actividad esté basada en el respeto a las leyes y a las normas vigentes en cada momento, así como en la promoción y defensa de sus valores corporativos y principios de actuación establecidos en su Código Ético y, por consiguiente, enlaza con sus valores éticos, ratificando la firme voluntad por mantener una conducta de estricto cumplimiento en materia de privacidad y uso ético de los datos y los componentes de inteligencia artificial.
- Establecer un marco general para la gestión de la privacidad y la protección de datos de carácter personal y uso ético de los datos y los componentes de inteligencia artificial, adaptándolo a las nuevas disposiciones normativas. El marco comprenderá el conjunto de medidas dirigidas a la prevención, detección y reacción e identificará los riesgos de privacidad y controles asociados a los mismos que se establezcan.
- Asegurar ante los accionistas, clientes, proveedores, organismos supervisores y la sociedad en general, que la Entidad y su Grupo cumplen con los deberes de supervisión y control de su actividad en relación con la privacidad y uso ético de los datos y los componentes de inteligencia artificial, estableciendo medidas adecuadas para prevenir o reducir el riesgo de actuaciones no respetuosas con la normativa vigente y que, por tanto, se ejerce el debido control legalmente procedente sobre administradores, directivos, empleados y demás personas asociadas.

El contenido de esta Política a la que se refieren estos principios incluye:

- Estrategia o principios generales que rigen la gestión de la privacidad y la protección de datos
- Marco de gobierno
- Marco de gestión en materia de privacidad, la y protección de datos y uso ético de los datos y los componentes de inteligencia artificial:
 - o Delegado de protección de datos (en adelante, DPO) y otras figuras responsables
 - o Tratamientos y legitimación
 - o Derechos de los interesados

- Evaluaciones de impacto
- Medidas técnicas
- Proveedores
- Comunicación y formación
- Marco de control
- Marco de *reporting* / información

2. *Ámbito de aplicación*

La Política a la que se refieren estos principios tiene carácter corporativo. En consecuencia, los principios de actuación definidos son aplicables a todas las sociedades del Grupo CaixaBank con exposición al riesgo de protección de datos y al uso ético de los datos y los componentes de inteligencia artificial. Los órganos de gobierno de estas sociedades adoptarán las decisiones oportunas con el objeto de integrar las disposiciones de la Política a la que se refieren estos principios adaptando, siguiendo el principio de proporcionalidad, el marco de gobierno a la idiosincrasia de su estructura de órganos de gobierno, comités y departamentos, y sus principios de actuación, metodologías y procesos a lo descrito en este documento.

Esta integración podrá suponer, entre otras decisiones, la aprobación de una política propia por parte de la filial. La aprobación será necesaria en aquellas filiales que precisen adaptar lo dispuesto en la Política a la que se refieren estos principios a sus especificidades propias, ya sea por materia, por jurisdicción o por relevancia del riesgo en la filial. En aquellos casos en los que las actividades de control y gestión del riesgo de la filial se realice directamente desde CaixaBank, ya sea por materialidad del riesgo en la filial, por razones de eficiencia o porque la filial haya externalizado en CaixaBank la gestión operativa de este riesgo, los órganos de gobierno de las filiales afectadas al menos tomarán conocimiento de la existencia de la Política corporativa a la que se refieren estos principios y de su aplicación a dichas filiales.

En cualquier caso, la Dirección de Compliance de CaixaBank, dado su carácter corporativo, velará por que la integración de esta Política en las filiales sea proporcionada, que en caso de que las filiales aprueben políticas propias estas estén alineadas con la política corporativa, y por la consistencia en todo el Grupo CaixaBank.

Por último, la Política a la que se refieren estos principios, además de ser corporativa, tiene la consideración de política individual de CaixaBank, matriz del Grupo CaixaBank.

3. Marco normativo. Normativa y estándares de aplicación

La Política a la que se refieren estos principios se regirá por lo previsto en la normativa aplicable vigente, así como por aquella que la modifique o sustituya en el futuro. En concreto, a fecha de su elaboración, la normativa vigente aplicable a la matriz del Grupo es la siguiente:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales

En el caso de filiales o, en su caso, sucursales sujetas a jurisdicciones extranjeras o normativa sectorial complementaria, las políticas y procedimientos que estas filiales o sucursales desarrollen tendrán en cuenta, además de su normativa propia, las obligaciones contenidas en la normativa antes referenciada en tanto no sean contradictorias con los requisitos específicos de la jurisdicción o normativa sectorial correspondiente.

Finalmente, en cada una de las sociedades del Grupo o, en su caso, sucursales, se desarrollarán los marcos, normas, guías o procedimientos que sean necesarios para la correcta implementación, ejecución y cumplimiento de la Política a la que se refieren estos principios.

4. Principios generales de la gestión de la privacidad

Los principios que orientarán la toma de decisiones del Grupo CaixaBank en materia de privacidad y protección de datos son los que siguen:

- **Tratamiento de los datos de manera lícita, leal y transparente.** Se respetará el ordenamiento jurídico de aplicación, el tratamiento de los datos personales se realizará siempre al amparo de alguna de las condiciones legales que lo permiten y se informará al Interesado al respecto incluyendo, en su caso, información sobre la elaboración de perfiles y sus consecuencias.
- **Tratamiento de los datos para fines determinados, explícitos y legítimos.** No se tratará la información para fines incompatibles con aquellos de los que se hayan informado al Interesado.
- **Tratamiento únicamente los datos adecuados, pertinentes y limitados** a cada finalidad del tratamiento.
- **Tratamiento de datos exactos y actualizados.** Se adoptarán las medidas que permiten suprimir o modificar la información, de forma que se mantenga exacta y al día.
- **Conservación de los datos únicamente durante el tiempo necesario.** En la mayoría de casos, los datos dejan de ser necesarios cuando finaliza la relación contractual o de negocio (o cuando se retira el consentimiento para su uso). A partir de ese momento, se procederá a la adaptación y modificación de los tratamientos de datos correspondientes adecuándolos, en su caso, al nuevo título habilitante (tales como el cumplimiento de obligaciones legales o para la formulación, el ejercicio o la defensa de sus derechos e intereses) y finalmente, se suprimirán.
- **Tratamiento de datos con garantía de seguridad.** La seguridad de la información es esencial. Por ello se protegerá contra tratamientos no autorizados o ilícitos y contra su pérdida, destrucción o daño accidental.
- **Actuación con responsabilidad proactiva.** CaixaBank se dotará de los procedimientos y herramientas necesarios para documentar y conservar todas las acciones que lleven a cabo, de conformidad con la Política y la normativa de protección de datos, en relación con los tratamientos que realizan, a los efectos no sólo de cumplir proactivamente con la normativa vigente, sino también para estar, en todo momento, en disposición de acreditar su cumplimiento.

5. Marco de gobierno

Los pilares sobre los que se asienta el marco de gobierno del riesgo de protección de datos y privacidad en el Grupo CaixaBank son:

- Cumplimiento de los principios recogidos en la Política a la que se refieren estos principios por parte de las sociedades del Grupo CaixaBank dentro de su ámbito de aplicación.
- Supervisión corporativa de la entidad matriz.
- Alineación de estrategias entre las sociedades del Grupo, y a su vez alineación con las mejores prácticas, con las expectativas supervisoras y con la regulación vigente.
- Implicación máxima de los órganos de gobierno y dirección de las sociedades del Grupo.
- Marco de control interno basado en el modelo de Tres Líneas de Defensa que garantiza la estricta segregación de funciones y la existencia de varias capas de control independiente.

6. Marco de gestión para la privacidad y la protección de datos

6.1 Delegado de Protección de Datos (DPO)

Es el asesor y supervisor del cumplimiento de la normativa sobre privacidad. Depende funcionalmente del DPO Corporativo, al que reporta y con el que se coordina. Sus responsabilidades, obligaciones, y pautas de funcionamiento se detallan a continuación.

6.1.1 Nombramiento

Es responsabilidad del Comité de Dirección de la Entidad el nombramiento del Delegado de Protección de Datos, así como el seguimiento de su desempeño. Se nombrará al Delegado de Protección de Datos:

- Atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados en derecho, la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que se le asignan.
- Con vocación de grupo, por lo que las sociedades del grupo establecidas en España que adopten la presente Política como propia, deberán nombrar como Delegado de Protección de Datos al Delegado de Protección de Datos de CaixaBank.
- Con carácter corporativo, ya que el Delegado de Protección de Datos de CaixaBank será el Delegado Corporativo de Protección de datos, del que dependerán funcionalmente los Delegados de Datos de las Empresas del Perímetro y los que pudieran nombrarse en otras jurisdicciones distintas a la española.

El nombramiento del Delegado de Protección de Datos se publicará y se comunicará a la autoridad de control.

6.1.2 Encaje organizativo y funciones

La Entidad garantizará, en todo momento, que el Delegado de Protección de Datos:

- Participa de forma adecuada y en tiempo oportuno en todas las cuestiones de protección de datos.

- Dispone de los recursos necesarios para el desempeño de sus funciones y el mantenimiento de sus conocimientos especializados y recibe formación adecuada.
- Tiene el acceso a los datos personales y operaciones objeto de tratamiento.
- Rinde cuentas directamente al más alto nivel jerárquico.
- Goza de independencia en el ejercicio de sus funciones.

El Delegado de Protección de datos, desempeñará, como mínimo, las siguientes funciones:

- Asesorar, informar y supervisar acerca del cumplimiento en las siguientes áreas/materias:
 - o Aplicación de los principios relativos al tratamiento de los datos personales.
 - o Identificación y aplicación de las bases jurídicas del tratamiento.
 - o Compatibilidad de finalidades distintas de las que originaron la recogida.
 - o Normativa sectorial que pueda afectar al tratamiento de los datos personales.
 - o Información a los afectados.
 - o Ejercicio de derechos de los Interesados.
 - o Contratación de encargados.
 - o Transferencias internacionales de datos.
 - o Política de protección de datos.
 - o Concienciación a los empleados y la organización.
 - o Formación a los empleados.
 - o Auditoría de protección de datos.
 - o Registros de actividades de tratamiento.
 - o Protección de datos desde el diseño.
 - o Análisis de riesgo de los tratamientos.
 - o Medidas de seguridad adecuadas.
 - o Violaciones de seguridad.
 - o En su caso, garantías para el responsable.
- Actuar como mediador entre los clientes y La Entidad en las reclamaciones sobre protección de datos.
- Cooperar y actuar como punto de contacto entre La Entidad y la AEPD u otra autoridad de control, para cuestiones relativas al tratamiento y realizar consultas sobre cualquier otro asunto.
- Actuar como punto de contacto para los Interesados y el ejercicio de derechos por su parte.

El Delegado de Protección desarrollará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento y teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

6.1.3 Facultades

En el desarrollo de sus funciones el Delegado de Protección de Datos tiene atribuidas las siguientes facultades:

- Acceder a la información y a los datos personales de los Interesados.
- Acceder a las operaciones del tratamiento automatizadas y no automatizadas.

- Consultar documentación, sistemas, programas, bases de datos, y en general cualquier soporte relativo a los datos personales o a su tratamiento.
- Participar en reuniones en las que se aborden cuestiones relativas a los tratamientos de datos personales.
- Mantener la interlocución con la AEPD y con otras autoridades de control.
- Tener acceso directo y reportar periódicamente a la alta dirección,.
- Organizar internamente sus recursos.

6.1.4 Independencia

La Entidad no impartirá instrucciones, sancionará o destituirá al DPO por el desempeño de sus funciones. Lo anterior se entiende sin perjuicio de la facultad organizativa que le asiste.

El Delegado de Protección de Datos tiene acceso y rinde cuentas al más alto nivel jerárquico.

6.1.5 Disponibilidad y participación efectiva

La Entidad se asegurará de que el DPO está disponible para sus funciones internas y externas y participa efectivamente en los análisis y valoraciones acerca de tratamientos de datos personales.

6.1.6 Dotación de medios

El Delegado de Protección de Datos en el desarrollo de sus funciones contará con los medios organizativos necesarios para desarrollar su actividad y, contará con el soporte interno legal y regulatorio de La Entidad para ello. También podrá recurrir a la contratación de asesores externos para aquellos temas que, a su juicio, resulten necesarios.

Para el desarrollo correcto de sus atribuciones, el DPO deberá contar con medios adecuados para, al menos, desarrollar las siguientes funciones básicas:

- Asesorar y dar soporte a la Entidad mediante la actualización de la normativa de aplicación en protección de datos y en la detección de posibles situaciones de riesgo de cumplimiento.
- Asesorar y dar asistencia a la Entidad mediante la interpretación de normas y aportando conocimiento y análisis de la normativa vigente y de los proyectos normativos en curso con el fin de prever su impacto en La Entidad.
- Asesorar en la supervisión y en particular en el diseño de controles de primer nivel.
- Asesorar y dar soporte en la formación de los empleados en materia de protección de datos.
- Asesorar y dar soporte a la tercera línea de defensa en la realización de controles periódicos en materia de protección de datos.
- Coordinar, asesorar y dar soporte en la realización de PIAs.

6.1.7 Comunicación interna y externa en materia de privacidad

El DPO tendrá acceso a los instrumentos de comunicación existentes en la Entidad al objeto de fomentar la cultura de cumplimiento. En esta tarea contará asimismo con la colaboración de aquellas áreas que tengan responsabilidades en el ámbito de la comunicación interna. A tal efecto:

- Las páginas web de la Entidad contendrán una referencia al Delegado de Protección de Datos.
- El Delegado de Protección de Datos dispondrá de una sección dentro de la intranet de la Entidad en la que aparecerá la Política de Privacidad así como cualquier otra información que el DPO considere necesaria para el adecuado desarrollo de sus funciones.

[6.1.8 Relaciones con las funciones de control](#)

A los efectos de que el Delegado de Protección de Datos pueda cumplir con las funciones establecidas en la normativa, así como en la presente Política, sus relaciones con otras funciones de control (Cumplimiento Normativo, Auditoría Interna, Gestión de Riesgos) se guiarán por los principios de cooperación e información recíproca.

Las áreas de control actuarán independientemente y bajo sus propios criterios, según se establezca en cada momento en la Política de Control Interno de La Entidad y mantendrán coordinación con el Delegado de Protección de Datos, facilitándose mutuamente la información necesaria para la adecuada supervisión y control del cumplimiento del derecho de protección de datos.

Sin perjuicio de lo anterior y en relación con las facultades de supervisión del cumplimiento de la normativa de protección de datos:

- El DPO asesorará a la primera línea de defensa en relación con los controles a implementar en sus respectivas áreas en relación con el cumplimiento de la normativa de protección de datos, siendo las correspondientes áreas o departamentos los encargados de su establecimiento y seguimiento.
- La supervisión del DPO del cumplimiento de la normativa de protección de datos se concretará en la definición e implementación de controles aleatorios y en función del riesgo de los tratamientos y contemplará tanto la supervisión de los aspectos jurídicos como de los aspectos técnicos y de Seguridad de la Información.

[6.1.9 El Delegado de Protección de Datos Corporativo](#)

Ostentará la condición de Delegado de Protección de Datos Corporativo el Delegado de Protección de Datos de CaixaBank, y tendrá como responsabilidades, adicionales a las propias en su condición de DPO de CaixaBank y de las Empresas del Perímetro que le nombren:

- Establecer las directrices generales para garantizar la adecuada gestión del riesgo de cumplimiento de la normativa de protección de datos y la implantación de la cultura de cumplimiento en relación con la misma en el Grupo. Asimismo, le corresponde establecer las directrices generales a los efectos de garantizar una interpretación homogénea de la norma en el Grupo
- Proponer la creación de órganos colegiados con alcance de grupo
- Promover el desarrollo de un marco de relaciones con los equipos de las empresas del grupo
- Comunicar todos aquellos aspectos que sean de interés (lecciones aprendidas, mejores prácticas, etc...) en las empresas del grupo
- Participar en el nombramiento y, en su caso, en el cese de los DPO nacionales de manera que propuesto el o los candidatos o el cese y sus motivos, el DPO Corporativo procederá a remitir su informe

- Participar, en lo que se refiere a la fijación de retos, evaluación del desempeño y determinación de la remuneración fija y variable de los DPO nacionales, para lo que la sociedad con presencia en el extranjero informará al DPO Corporativo con carácter previo a la adopción de las correspondientes decisiones debiendo este último remitir su informe a la filial
- Participar y conocer toda comunicación regular con los supervisores locales por parte de las sociedades del grupo
- Participar y conocer en todo momento el estado de la gestión de la privacidad en las sociedades del grupo

6.1.10 Modelo de Gobierno de la función de DPO en la presencia internacional

CaixaBank como cabecera de un grupo que presta servicios financieros y de inversión tiene una vocación internacional y se ha establecido en otras jurisdicciones, fuera y dentro de la Unión Europea, a través de sucursales y oficinas de representación. Asimismo, el Grupo CaixaBank tiene presencia en otras jurisdicciones a través de filiales o en libre prestación de servicios.

- En el primer caso, la presencia de CaixaBank en jurisdicciones fuera y dentro de la Unión Europea mediante la apertura de sucursales y oficinas de representación de CaixaBank, el Delegado de Protección de Datos es el de CaixaBank, S.A. al no tener dichas estructuras personalidad jurídica propia.
- En el segundo de los casos, la presencia a través de filiales o en régimen de libre prestación de servicios, las mencionadas sociedades del Grupo establecidas fuera de España, deberán –para el caso que así lo requiera la normativa- nombrar a un Delegado de Protección de datos nacional que cumpla con las siguientes obligaciones que el RGPD establece:
 - o Que el DPO debe ser experto en la práctica en materia de protección de datos y necesita, en consecuencia, de un conocimiento experto en cada jurisdicción,
 - o Que el DPO debe actuar como punto de contacto y colaborar con la Autoridad de control
 - o Que el DPO debe ser fácilmente accesible por los titulares de los datos desde cada establecimiento (y, en consecuencia, resulta necesario que tenga un conocimiento alto del idioma local)

6.2 Otras figuras responsables

6.2.1 Responsable de Privacidad

Figura responsable del control y cumplimiento de la normativa de privacidad en cada una de las sociedades del Perímetro nombrado por los órganos de gobierno o dirección de cada una de las mismas. El Responsable de Privacidad será el máximo responsable de la gestión de la privacidad en su organización. A estos efectos, se coordinará con el Delegado de Protección de Datos.

Ostentará la condición de Responsable de Privacidad quien así haya sido nombrado por el Comité de Dirección de la sociedad. En defecto de nombramiento expreso lo será el Presidente del Comité de Privacidad de la compañía.

6.2.2 *Coordinador de Privacidad de las Áreas o Direcciones Territoriales*

Figura encargada de asesorar en el cumplimiento de la normativa de protección de datos y realizar las PIAs en las áreas, departamentos, líneas de negocio o direcciones territoriales de la Entidad. Asimismo, es el punto de coordinación y contacto de su ámbito con el DPO.

6.3 *Tratamientos y Legitimación*

La Entidad tratará los datos personales de los Interesados para las siguientes finalidades:

- “Precontractuales” o “contractuales”: para atender solicitudes en relación con sus servicios y prestarlos con arreglo a la calidad que se espera. La actividad de CaixaBank, como entidad de crédito, requiere que se obtenga determinada información, se analice, conserve, actualice, y acceda a ella, en respuesta a quienes se interesan o piden los servicios a la Entidad. También se necesita tratar la información de los candidatos y empleados para, en su caso, entablar una relación laboral o gestionarla. Lo mismo sucede en el caso de la relación mercantil que mantiene con sus proveedores.
- “Regulatorias o normativas”: para cumplir las obligaciones exigidas por las diferentes normativas, políticas y códigos, como, por ejemplo: la adopción de medidas de diligencia debida en la prevención del blanqueo de capitales y de la financiación del terrorismo, fiscal, de prevención del fraude, sanciones internacionales o aquellas obligaciones de reporte requeridas por las autoridades reguladoras del sector financiero.
- “Comerciales”: La Entidad puede tratar los datos con dicha finalidad basado en el interés legítimo o previa autorización del titular del dato (consentimiento).
- “Organizativos y de prevención del fraude”: La Entidad puede tratar los datos con dicha finalidad según la necesidad para la ejecución de las relaciones contractuales, la obligación legal o el interés legítimo.

6.4 *Derechos de los interesados*

La Entidad facilita a los Interesados el ejercicio de sus derechos según se definen en la normativa de protección de datos.

Para ello, La Entidad se ha dotado de los procedimientos, así como de las herramientas y recursos necesarios para realizar una gestión centralizada de los derechos que le permita facilitar a los interesados el ejercicio de éstos mediante canales físicos como digitales. El detalle de estos procedimientos se reflejará actualizado en la Norma de Privacidad de La Entidad.

6.5 *Evaluaciones de impacto*

Entre los requerimientos y obligaciones que establece el RGPD destaca la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de los datos personales siempre y cuando sea probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas (PIA).

En este sentido, La Entidad se ha dotado de un procedimiento, así como de una metodología para la realización de las mencionadas evaluaciones de impacto.

Este procedimiento se basa en el principio de que todos los tratamientos que se realicen deben ser detallados por su promotor, debe hacerse una evaluación de sus riesgos, y las medidas necesarias para mitigarlos y la decisión sobre la viabilidad del tratamiento propuesto debe ser sancionada por el Comité correspondiente.

El detalle de estos procedimientos se reflejará actualizado en la norma de privacidad de La Entidad.

6.6 Medidas técnicas

La Entidad aplica las medidas técnicas y organizativas necesarias para mitigar los riesgos asociados con la protección de la información personal y de los derechos y libertades de los Interesados.

Las medidas generales destinadas a evitar los riesgos sobre la alteración, pérdida, indisponibilidad y tratamiento o acceso no autorizado a la información se describen en la Política de Seguridad de la Información del Grupo CaixaBank. Desde un enfoque preventivo y proactivo se definen las medidas a aplicar en los sistemas de información para proteger la información en todo su ciclo de vida. En cualquier caso, la aplicación de las medidas concretas será consecuencia del análisis y evaluación del riesgo específico para cada tratamiento, siguiendo la metodología prevista para las Evaluaciones de Impacto (PIAs).

Además, la Entidad y las sociedades del Grupo CaixaBank, aplican un procedimiento común para la gestión de las brechas o violaciones de seguridad de los datos personales de acuerdo a la Política de Seguridad de la Información del Grupo CaixaBank. Dicho procedimiento incluye el registro, gestión y notificación de las violaciones de seguridad de los datos personales a la AEPD y, cuando un entrañe un alto riesgo para los derechos y libertades, también al Interesado.

6.7 Proveedores

La Entidad se ha dotado de los procedimientos, así como de las normas internas necesarias para realizar una selección responsable de sus proveedores de acuerdo con lo que establece la normativa de protección de datos de carácter personal.

Los procedimientos de contratación de Proveedores y los contratos de prestación de servicios de La Entidad incorporan requerimientos específicos en el caso de que la prestación de servicios correspondiente implique el tratamiento de datos personales, así como medios de seguimiento y control de los proveedores.

6.8 Comunicación y formación

Para la Entidad es fundamental que sus empleados, clientes y accionistas conozcan el derecho a la protección de datos y sean conscientes de la importancia que para la Entidad tiene la confidencialidad y el respeto al derecho fundamental de la protección de datos de carácter personal de los titulares de los datos.

Por ello la Entidad imparte formación periódicamente a sus empleados sobre protección de datos.

Adicionalmente, la Entidad lleva a cabo campañas de concienciación periódicas a los efectos de reforzar el mensaje acerca de la importancia de cumplir con la normativa y las obligaciones derivadas de ésta y de la presente Política.